IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

DAVID JACOB, Individually and on Behalf of All Others Similarly Situated, Plaintiff, v. AMERICAN NEIGHBORHOOD MORTGAGE ACCEPTANCE COMPANY, LLC D/B/A ANNIEMAC HOME MORTGAGE, Defendant.	Case No. _____ **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff David Jacob ("Plaintiff" or "Jacob") brings this Class Action Complaint ("Complaint") against American Neighborhood Mortgage Acceptance Company, LLC d/b/a AnnieMac Home Mortgage ("AnnieMac" or "Defendant"), individually and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigation, and upon information and belief as to all other matters, as follows:

SUMMARY OF THE ACTION

1. This is a class action on behalf of individuals who had their personally identifying information ("PII") stolen by hackers as part of a major data breach which occurred in or around August 2024, and which affected Defendant's network.

2. Defendant is a "nationwide mortgage loan provider dedicated to the principle of service — to our clients, our employees, and our business partners."[1] It is "headquartered in

[1] https://www.linkedin.com/company/anniemac-home-mortgage/

Mount Laurel, N.J." but has "branches throughout the country that employ hundreds more."[2] It has "emerged as one of the fastest-growing home lenders in the industry."[3]

3. Accordingly, in the course of conducting its regular business, Defendant stores a copious amount of highly sensitive PII about its former and current customers, as well as applicants for home loans, including Plaintiff's and Class Members' PII. However, due to its negligent conduct in improperly maintaining or otherwise failing to adhere to standard cybersecurity protocols, Defendant lost control over Plaintiff's and Class Members' PII when cybercriminals infiltrated its computer systems in a data breach (the "Data Breach").

4. The PII compromised in the Data Breach included Plaintiff's and Class Members' names and Social Security numbers.

5. By taking possession and control of Plaintiff's and Class Members' PII as a condition of providing account administration and processing services for Plaintiff and Class Members, Defendant impliedly assumed a duty to refrain from committing acts or omissions that had a substantial likelihood of resulting in reasonably foreseeable harm to Plaintiff's and Class Members' data security by implementing and maintaining adequate and reasonable cybersecurity procedures and protocols to protect Plaintiff's and Class Members' PII from unauthorized disclosure.

6. Furthermore, Defendant had a statutory duty to adequately safeguard the PII of Plaintiff and Class Members imposed by Section 5 of the Federal Trade Commission Act of 1914 ("FTC Act"), which prohibits "unfair … practices in or affecting commerce." The Federal Trade Commission ("FTC") has interpreted Section 5 of the FTC act as providing liability

[2] *Id.*
[3] *Id.*

against companies for failing to use reasonable measures to protect PII. *See In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 408 (E.D. Va. 2020).

7. Defendant breached its duty to Plaintiff and Class Members when it failed to implement and maintain adequate cybersecurity procedures and protocols to safeguard Plaintiff's and Class Members' PII, resulting in the unauthorized disclosure of Plaintiff's and Class Members' PII to cybercriminals.

8. But for the Defendant's failure to implement and maintain reasonable cybersecurity protocols and procedures, Plaintiff's and Class Members' PII would not have been inadvertently disclosed to hackers, making Defendant's actions a factual cause of the unauthorized disclosure.

9. Defendant also proximately caused the unauthorized disclosure because the actions of third-party bad actors such as by cybercriminals do not constitute a superseding force that would relieve Defendant of liability because misappropriation of PII for unlawful purposes by cybercriminals is a reasonably foreseeable result of an unauthorized disclosure of PII.

10. The damages suffered by Plaintiff and Class Members due to the Data Breach are substantial. The unauthorized online disclosure of an individual's PII through a data breach exposes that individual to an increased risk of identity theft as online, third-party bad actors may access the PII to commit a number of frauds against the individuals, including, but not limited to: opening fraudulent credit cards in the ID theft victim's name, stealing government benefits rightfully belonging to the victims, applying for loans in the victims' names, and accessing the victims' bank accounts.

11. As such, individuals who have had their PII disclosed to cybercriminals must spend time and money to ameliorate the detrimental effects of the breach, usually by closely monitoring their financial accounts for unauthorized activity, contacting the three major U.S. credit reporting agencies to obtain a credit report, and placing a fraud alert on their credit file. Furthermore,

individuals who have had their PII disclosed in a data breach may need to continue performing these ameliorative actions for the rest of their lives, costing an unascertainable amount in lost time and money. In fact, mitigation of the misuse of PII stolen in a data breach may not even be possible.

12. Thus, Plaintiff seeks to remedy these harms on behalf of himself and all other similarly situated individuals whose PII was stolen in the Data Breach. Plaintiff asserts claims for negligence, negligence per se, unjust enrichment, and invasion of privacy and seek: (i) monetary damages; (ii) punitive damages; (iii) fees and costs of litigation; (iv) injunctive relief, including the adoption of reasonably sufficient practices to safeguard PII in Defendant's custody, care, and control in order to prevent incidents like the Data Breach from recurring in the future and for Defendant to provide long-term identity theft protective services and credit monitoring to Plaintiff and class members; (v) disgorgement; and (v) such other relief as the Court deems just and proper.

PARTIES

A. Plaintiff

13. Plaintiff David Jacob is a natural person and a resident and citizen of Cherry Hill, New Jersey.

B. Defendant

14. Defendant American Neighborhood Mortgage Acceptance Company, LLC d/b/a AnnieMac Home Mortgage is a nationwide mortgage loan provider. Defendant is organized and exists under the laws of the State of Delaware and has its principal place of business located at 700 East Gate Drive, Suite 400, Mount Laurel, New Jersey 08054. Defendant, thus, is a citizen of Delaware and New Jersey.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because at least one member of the putative class, as defined below, is a citizen of a state other than that of Defendant, there are more than 100 putative class members, and the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs.

16. This Court has general personal jurisdiction over Defendant because it maintains its principal place of business in this judicial district, regularly conducts business in this judicial district, and the acts and omissions giving rise to Plaintiff's claims emanated from within this judicial district.

17. Venue in this district is proper under 18 U.S.C. §1391(b) because Defendant maintains its principal place of business in this judicial district, and a substantial part of the acts and omissions giving rise to Plaintiff's claims occurred in this district, including Defendant's collecting and storing of the PII of Plaintiff and putative Class Members.

FACTUAL BACKGROUND

A. Defendant Collects, Stores, and Maintains Huge Amounts of Personally Identifiable Information

18. Defendant is a corporation that provides mortgage loan services to home borrowers.

19. Plaintiff and Class Members are current and former customers or applicants for mortgage loan services provided or administered by Defendant.

20. When Plaintiff and Class Members applied for home mortgage loan services with AnnieMac, they were required to hand over their PII to Defendant including their names and Social Security numbers.[4]

21. However, according to Defendant's privacy policy, the types of PII it collects on its consumers can be even more extensive and can come from a variety of sources other than the consumers themselves. As AnnieMac explains, "During the course of processing your application, we accumulate non-public personal financial information from you and from other sources about your income, your assets, and your credit history in order to allow a lender to make an informed decision about granting you credit."[5]

22. Such PII can include:

- Usernames and passwords
- Contact information (such as names, email addresses, mailing addresses, and telephone numbers)
- Financial account information
- Payment card information
- Social Security numbers
- Driver's license numbers (or comparable)
- Photographs or fingerprints
- Information provided through the services (e.g., feedback, inquiries, etc.)
- Communications with AnnieMac, such as emails, call recordings, or messages

[4] California Consumer Privacy Act Policy, ANNIEMAC, https://www.annie-mac.com/page/capp (last visited November 23, 2024).
[5] Privacy Policy, ANNIEMAC, https://www.annie-mac.com/page/privacy

- Transactional information associated with lending and other financial services (including information relating to account management, deposits, withdrawals and other financing and lending activities)
- Mobile activity (including unique device identifiers or other device information, mobile phone numbers, and general locations.[6]

23. According to AnnieMac's privacy policy, this information may also come from additional online and offline sources and third parties (e.g., credit reporting agencies) to supplement the information provided by consumers.[7]

24. Given the vast scope of the variety of sources AnnieMac pulls from to collect information on consumers, including Plaintiff and Class Members, it can be nearly impossible for Plaintiff or any single Class Member to ascertain exactly how much PII that AnnieMac has collected from them and negligently disclosed in the Data Breach without further discovery. Thus, Defendant cannot simply relieve itself of liability for negligently disclosing such data by requiring Plaintiff to plead the exact amount and/or exact nature of the data that was disclosed in the Data Breach.

25. Furthermore, in its privacy policy, Defendant makes assurances to consumers that it "restrict[s] access to nonpublic personal information about you to those employees who need to know that information to provide products or services to you."[8] It also represents that it "maintain[s] physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information."[9]

---

[6] California Consumer Privacy Act Policy, ANNIEMAC, https://www.annie-mac.com/page/capp (last visited November 23, 2024).
[7] *Id.*
[8] Privacy Policy, ANNIEMAC, https://www.annie-mac.com/page/privacy
[9] *Id.*

26. Thus, AnnieMac collected consumers' PII, and in collecting and maintaining consumers' PII—including the PII of Plaintiff and Class Members, it agreed it would safeguard that data in accordance with internal policies, federal law, state law, and common law duties.

B. The Data Breach

27. On or around November 14, 2024, Jacob received a "Notice of Security Incident" letter from Defendant (the "Data Breach Letter").

28. According to the Data Breach Letter, on August 23, 2024, AnnieMac "became aware of suspicious activity on certain systems within our network." In the same letter, AnnieMac informed the Plaintiff that "an investigation into the nature and scope of the event … determined that between August 21, 2024 and August 23, 2024, an unknown actor gained access to our systems and viewed and/or copied certain files from these systems."

29. The Data Breach Letter further notified Plaintiff that "the investigation determined certain information related to you was contained within the affected files." That information included at least "your name and Social Security number," which AnnieMac disclosed "were present within the affected files."

30. However, this "Notice of Data Security Incident" was hardly notice at all as it intentionally obfuscated important facts about the Data Breach from the Plaintiff and similarly affected consumers, including Class Members.

31. For example, Defendant does not disclose in the Data Breach Letter the identity of the cybercriminals who perpetrated the Data Breach. Furthermore, the Defendant does not the details of the cause or causes of the Data Breach. To date, such omitted and material details have not been disclosed to Plaintiff or Class Members.

32. These undisclosed facts are material to Plaintiff and Class Members who needed them in order to mitigate the harms resulting from the Data Breach and retain a vested interest in

ensuring their PII remains protected. Thus, the insufficient disclosures in the Data Breach letter constitute a separate and distinct harm from the Data Breach itself because it has prevented Plaintiff and Class Members from taking timely steps to mitigate their own damages. Despite the Defendant's intentional obfuscation of the material facts of the Data Breach, what can still be gleaned from the Data Breach Letter include the following facts:

a. The Data Breach was the work of cybercriminals

b. The cybercriminals infiltrated Defendant's computer systems and downloaded consumers' PII from those systems

c. Once inside Defendant's computer systems, the cybercriminals targeted Plaintiff's and Class Members' PII, including Social Security numbers, for download and theft.

33. Corporations only send such Data Breach Letters as was sent to Plaintiff in the instant case to those persons whose personal information the Defendant itself reasonably believes has been accessed or acquired by unauthorized individuals or entities. By sending the Data Breach Letter to Plaintiff and similarly affected consumers, Defendant admits it has a reasonable belief that the PII of Plaintiff and Class Members was accessed or otherwise acquired by unauthorized individuals or entities—i.e., cybercriminals.

34. Although Defendant offers 12 months of credit monitoring and identity protection services to Plaintiff and similarly affected consumers in the Data Breach Letter, such an offer is an insufficient remedy for the harms sustained by Plaintiff and Class Members. That is because, (as explained in more detail below), the harms sustained by Plaintiff and Class Members is potentially irreversible and could last for the remainder of their lifetimes as they cannot control how the cybercriminals who have accessed their PII may continue to sell, or otherwise share, that data on black markets on Dark Web to other individuals and entities who may continue to use that information to commit frauds and identity theft against them.

35. In short, Defendant's failure to implement and maintain reasonable cybersecurity protocols and procedures constituted a negligent act and/or omission which deleteriously compromised the data security of Plaintiff and putative Class Members, which could potentially be irreversible and last for their respective lifetimes. Such harms include the diminution of the inherent monetary value of Plaintiff's and Class Members' undisclosed PII, but also the time and money Plaintiff and Class Members will have to spend to ameliorate the detrimental effects of having their PII disclosed online to cybercriminals, including and not limited to, closely monitoring their financial accounts and placing fraud alerts on all their financial accounts.

C. Companies Are Increasingly Susceptible to Data Breaches, Giving Defendant Ample Notice That They Are Likely Cyberattack Targets

36. Large companies like Defendant are well-aware of the numerous, large scale data breaches that have occurred throughout the United States and internationally, and of their responsibility for safeguarding the PII and other private customer information in their possession. Such breaches have become frequent and widespread. Thus, at all relevant times, Defendant knew, or should have known, that the PII and other private information it was entrusted with was a target for malicious actors. In particular, Defendant knew this given the unique type and the significant volume of data on its networks, software, servers, and systems, comprising individuals' detailed and confidential PII and, thus, the significant number of individuals who the exposure of the unencrypted data would harm. As custodian of Plaintiff's and Class Members' PII, Defendant knew or should have known the importance of protecting their PII, and of the foreseeable consequences and harms to such persons if any data breach occurred.

37. In 2023 alone, 3,205 data breaches occurred, resulting in more than 353 million individuals' sensitive records in the United States being exposed.[10] The 3,205 reported data

[10] Annual Number of Data Compromises and Individuals Impacted in the United States from 2005 to 2023, STATISTA, https://www.statista.com/statistics/273550/data-breaches-recorded-

breaches are a sharp increase from 2022, when 1,802 data breaches occurred.[11] With the surging number of such attacks, Defendant should have known that it was at a high risk of a cyberattack and should have taken additional and stronger precautions and preemptive measures.

38. Additionally, in light of recent high profile data breaches at other industry leading companies, including MOVEIt (90 million records, June 2023), LastPass/GoTo Technologies (30 million records, August 2022), Neopets (69 million records, July 2022), WhatsApp (500 million records, November 2022), Twitter (5.4 million records, July 2022), Cash App (8.2 million users, April 2022), LinkedIn (700 million records, April 2021), Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estée Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), Advanced Info Service (8.3 billion records, May 2020), and others, Defendant knew or should have known that the PII that it collected and maintained would also be specifically targeted by cybercriminals.

D. Defendant Breached Its Duties to Plaintiffs and the Class, and Failed to Comply with Regulatory Requirements and Industry Best Practices

39. Because Defendant was entrusted with PII and other private information at all times herein relevant, Defendant owed to Plaintiff and the Class a duty to exercise commercially reasonable methods and care in handling, using, maintaining, storing, and safeguarding the PII in its care, control, and custody, including by implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use

---

inthe-united-states-by-number-of-breaches-and-records-exposed/ (last visited February 20, 2024).

[11] *See id.*

that occurred, and to promptly detect and thwart attempts at unauthorized access to its networks and systems. Defendant also owed a duty to safeguard PII and other private information because it was on notice that it was handling highly valuable data and knew there was a significant risk it would be targeted by cybercriminals. Furthermore, Defendant knew of the extensive, foreseeable harm that would ensue for the victims of a data breach, and therefore also owed a duty to reasonably safeguard that information.

40. Security standards commonly accepted among businesses like Defendant that store PII and other private information include, without limitation:

i. Maintaining a secure firewall configuration;

ii. Monitoring for suspicious or irregular traffic to servers or networks;

iii. Monitoring for suspicious credentials used to access servers or networks;

iv. Monitoring for suspicious or irregular activity by known users;

v. Monitoring for suspicious or unknown users;

vi. Monitoring for suspicious or irregular server requests;

vii. Monitoring for server requests for PII or other private information;

viii. Monitoring for server requests from VPNs; and

ix. Monitoring for server requests for Tor exit nodes.

41. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity[12] and protection of PII which includes basic security standards applicable to all types of businesses.[13]

42. The FTC recommends that businesses:

i. Identify all connections to the computers where sensitive information is stored.

ii. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

iii. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

iv. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

v. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hacker attacks.

vi. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

vii. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to

[12] Start with Security: A Guide for Business, FTC (June 2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[13] Protecting Personal Information: A Guide for Business, FTC (October 2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personalinformation.pdf.

allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

viii. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

ix. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business's network, the transmission should be investigated to make sure it is authorized.

43. As described further below, Defendant owed a duty to safeguard Plaintiff's and Class Members' PII and other private information under statute, including the FTC Act, to ensure that all information it received, maintained, and stored was secure. The FTC Act was enacted to protect Plaintiff and the Class Members from the type of conduct in which Defendant has engaged, and the resulting harms it proximately caused Plaintiff and the Class Members.

44. Under the FTC Act, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard the PII of Plaintiff and Class Members.

45. Defendant breached its duty to exercise reasonable care in protecting Plaintiff's and Class Members' PII by failing to (1) implement and maintain adequate data security measures to safeguard Plaintiff's and Class Members' sensitive personal information, (2) encrypt or anonymize PII within its systems and networks, (3) monitor its systems and networks to promptly identify and thwart suspicious activity, (4) delete and purge PII no longer necessary for its provision of telecommunications and software services to its clients and customers, (5) timely act upon data security warnings and alerts, (6) allowing unmonitored and unrestricted access to unsecured PII, (7) and allowing not preventing unauthorized access to, and exfiltration of, Plaintiff's and Class Members' confidential and private information. Additionally, Defendant

breached its duty by utilizing outdated and ineffectual data security measures which deviated from standard industry best practices at the time of the Data Breach. Through these actions, Defendant also violated its duties under the FTC Act.

46. Defendant failed to prevent the Data Breach, and had it properly maintained and adequately protected its software, systems, servers, and networks, the Data Breach would not have occurred.

47. Additionally, the law imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of PII to Plaintiff and class members so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuses of their PII. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and class members. In so doing, Defendant actually and proximately caused and exacerbated the harm from the Data Breach and the injuries-in-fact of Plaintiff and class members.

48. At all relevant times, Plaintiff and class members have taken reasonable steps to maintain the confidentiality of their PII.

E. Plaintiff's Experience

49. Plaintiff Jacob submitted an application for a mortgage to a mortgage broker, which on information and belief, provided his PII to AnnieMac a few years ago. In the course of completing his mortgage application, Plaintiff Jacob provided (and Defendant acquired) his PII, including his name, Social Security number, date of birth, contact information, financial information, location information, and other private and sensitive information.

50. Defendant admitted that, at least, his name and Social Security number were among the information stolen by an unknown actor during the Data Breach. Plaintiff is therefore a Data

Breach victim, as his PII and other private information was among the data accessed by unauthorized third parties in the Data Breach.

51. Plaintiff Jacob works hard to maintain an excellent credit score, and he is very worried that the data breach may result in identity theft, financial fraud, or other fraudulent activity that may negatively impact his credit score.

52. Plaintiff regularly monitors his financial accounts and will spend significant time monitoring his accounts due to the risk of identity theft, financial fraud, and other fraudulent activity. Plaintiff will spend time protecting himself from identity theft resulting from the Data Breach for the foreseeable future and beyond.

53. The Data Breach has caused Plaintiff Jacob to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

54. Plaintiff suffered actual injuries in the form of damages to and diminution in the value of his PII—a form of intangible property that was entrusted to Defendant, which was compromised as a proximate result of the Data Breach.

55. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from his PII and other private information being obtained by unauthorized third parties and very possibly cybercriminals.

56. Plaintiff has a continuing interest in ensuring that his PII and other private information, which remains within Defendant's possession and control, is protected and safeguarded against future data breaches and other cybersecurity risks.

57. Defendant deprived Plaintiff of the earliest opportunity to guard himself against the Data Breach's harmful effects by failing to promptly and/or adequately notify him about it.

F. Plaintiff and the Class Suffered Actual and Impending Injuries Resulting From the Data Breach

58. As a proximate result of Defendant's completely irresponsible security practices, identity thieves now possess the sensitive PII of Plaintiff and Class Members. It is well known that private information is valuable property. Once stolen, PII can be used in a number of different malicious ways. That information is extraordinarily valuable on the black market and incurs direct costs to Plaintiff and Class Members. Indeed, the link between a data breach and risk of identity theft is simple, well-established, and strong. On the Dark Web—an underground Internet black market—criminals openly buy and sell stolen PII to create "identity kits" worth up to $2,000 each that can be used to create fake IDs, gain access to bank accounts, social media accounts and credit cards, file false insurance claims or tax returns, or rack up other kinds of expenses.[14] And, "[t]he damage to affected [persons] may never be undone."[15]

59. Unlike simple credit card breaches at retail merchants, these damages cannot be avoided by canceling and reissuing plastic cards or closing an account. Identity theft is far more pernicious than credit card fraud. Criminals' ability to open entirely new accounts—not simply prey on existing ones—poses far more dangerous problems. Identity thieves can retain the stolen information for years until the controversy has receded because victims may become less vigilant in monitoring their accounts as time passes. Then, at any moment, the thief can take control of a victim's identity, resulting in thousands of dollars in losses and lost productivity. The U.S. Department of Justice has reported that in 2021 identity theft victims spent approximately four

[14] Nick Culbertson, *Increased Cyberattacks on Healthcare Institutions Shows the Need for Greater Cybersecurity* (June 7, 2021), FORBES, https://www.forbes.com/sites/forbestechcouncil/2021/06/07/ increased-cyberattacks-on-healthcare-institutions-shows-the-need-for-greatercybersecurity/?sh= ca928c05650d.

[15] *Id.*

hours on average to resolve problems stemming therefrom and that the average financial loss experienced by an identity theft victim was $1,160 per person.[16] Additionally, about 80% of identity theft victims reported some form of emotional distress resulting from the incident.[17]

60. Social Security numbers are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult to change. The Social Security Administration ("SSA") stresses that the loss of an individual's Social Security number can lead to identity theft and extensive financial fraud:

> Identity theft is one of the fastest growing crimes in America. A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, when they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought.
>
> Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[18]

61. Even when an injured person successfully goes through the cumbersome and time-consuming process of changing their Social Security number following identity theft, the SSA cautions individuals to "[k]eep in mind that a new number probably won't solve all your problems" and "can't guarantee you a fresh start."[19]

---

[16] Erika Harrell and Alexandra Thompson, Victims of Identity Theft, 2021, U.S. DEPARTMENT OF JUSTICE, OFFICE OF JUSTICE PROGRAMS, BUREAU OF STATISTICS (October 2023), *available at* https://bjs.ojp.gov/document/vit21.pdf.

[17] *Id.*

[18] Identity Theft and Your Social Security Number, U.S. SOCIAL SECURITY ADMINISTRATION (July 2021), *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf.

[19] *Id.*

62. Class Members' credit profiles can be destroyed before they even realize what has happened, and they may be unable to legitimately borrow money, obtain credit, or open bank accounts. Class Members can be deprived of legitimate tax refunds or, worse yet, may face state or federal tax investigations due to fraud committed by an identity thief. And even the simple preventive step of adding oneself to a credit-fraud watch list to guard against these consequences substantially impairs class members' ability to obtain additional credit. In fact, many experts advise victims to place a freeze on all credit accounts, making it impossible to rent a car, get student loans, buy or rent big-ticket items, or complete a major new car or home purchase.

63. Additionally, Class Members will spend significant amounts of time on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach and in navigating its effects.

64. Defendant's "security incident" notice provides hardly any compensation or relief whatsoever to affected persons for its wrongful conduct and actions described herein.

CLASS ACTION ALLEGATIONS

65. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiff seeks certification of the following nationwide class (the "Nationwide Class" or the "Class"):

> **All persons whose PII or other private information was compromised in the Data Breach disclosed by Annie Mac**

66. Excluded from the Nationwide Class are governmental entities, Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, affiliates, legal representatives, employees, co-conspirators, successors, subsidiaries, and assigns. Also excluded from the Nationwide Class are any judges, justices, or judicial officers presiding over this matter and the members of their immediate families and judicial staff.

67. This action is brought and may be properly maintained as a class action pursuant to Fed. R. Civ. P. 23(b)(2) and 23(b)(3) and satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of these rules.

68. *Numerosity Under Rule 23(a)(1)*. The Nationwide Class is so numerous that individual joinder of all members is impracticable, if not impossible, and the disposition of the claims of all members of the Nationwide Class in a single action will provide substantial benefits to the parties and the Court. Although the precise number of members of the Nationwide Class is unknown to Plaintiff at this time, on information and belief, potentially hundreds of thousands of people have been affected. Discovery will reveal, through Defendant's records, the number of members of the Nationwide Class.

69. *Commonality Under Rule 23(a)(2)*. Common legal and factual questions exist that predominate over any questions affecting only individual members of the Nationwide Class. These common questions, which do not vary among members of the Nationwide Class and which may be determined without reference to any Nationwide Class Member's individual circumstances, include, but are not limited to:

a. Whether Defendant knew or should have known that its computer systems, software, servers, and networks were vulnerable to unauthorized third-party access or a cyberattack;

b. Whether Defendant failed to utilize and maintain adequate and reasonable security and preventive measures to ensure that its computer systems, software, servers, and networks were protected;

c. Whether Defendant failed to take reasonably available steps to prevent and stop the Data Breach from occurring;

d. Whether Defendant owed a legal duty to Plaintiff and Class Members to protect their PII and other private information;

e. Whether Defendant breached any duty to protect the PII of Plaintiff and Class Members by failing to exercise due care in protecting their sensitive and private information;

f. Whether Defendant provided timely, accurate, and sufficient notice of the Data Breach to Plaintiff and the Class Members;

g. Whether Plaintiff and Class Members have been damaged by the wrongs alleged herein and are entitled to actual, statutory, or other forms of damages and other monetary relief; and

h. Whether Plaintiff and Class Members are entitled to injunctive or equitable relief, including restitution.

70. *Typicality Under Rule 23(a)(3)*. Plaintiff's claims are typical of the claims of the Nationwide Class. Plaintiff**,** like all proposed members of the Class, had his PII compromised in the Data Breach. Defendant's uniformly unlawful course of conduct injured Plaintiff and Class Members by way of the same wrongful acts and practices. Likewise, Plaintiff and other Class Members must prove the same facts in order to establish the same claims.

71. *Adequacy of Representation Under Rule 23(a)(4)*. Plaintiff is an adequate representative of the Nationwide Class because he is a Nationwide Class Member and his interests do not conflict with the interests of the Nationwide Class. Plaintiff has retained counsel competent and experienced in complex litigation and consumer protection class action matters such as this action, and his counsel intend to vigorously prosecute this action for the Nationwide Class's benefit and have the resources to do so. Plaintiff and his counsel have no interests adverse to those of the other members of the Nationwide Class.

72. *Predominance and Superiority*. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy because individual litigation of each Nationwide Class Member's claim is impracticable. The damages, harm, and losses suffered by the individual members of the Nationwide Class will likely be small relative to the burden and expense of individual prosecution of the complex litigation necessitated by

Defendant's wrongful conduct. Even if each Nationwide Class Member could afford individual litigation, the Court system could not. It would be unduly burdensome if millions of individual cases or more proceeded. Individual litigation also presents the potential for inconsistent or contradictory judgments, the prospect of a race to the courthouse, and the risk of an inequitable allocation of recovery among those individuals with equally meritorious claims. Individual litigation would increase the expense and delay to all parties and the Courts because it requires individual resolution of common legal and factual questions. By contrast, the class action device presents far fewer management difficulties and provides the benefit of a single adjudication, economies of scale, and comprehensive supervision by a single court.

73. As a result of the foregoing, class treatment under Fed. R. Civ. P. 23(b)(2) and (b)(3) is appropriate.

CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION
Negligence
(*On Behalf of the Plaintiff and the Nationwide Class Against Defendant*)

74. Plaintiff incorporates by reference and realleges paragraphs 1-73 as if fully set forth herein.

75. Without Plaintiff's or Class Members' consent, Defendant solicited, gathered, and stored the PII of Plaintiff and Class Members in the ordinary course of its business administering the various debt relief programs Plaintiff and Class Members were enrolled in. Upon information and belief, Defendant made representations and assurances to its customers that the PII Defendant collected and stored would be kept confidential, and that the privacy of the PII would be maintained. Because Defendant was entrusted with such PII at all times herein relevant, Defendant owed to Plaintiff and the Class Members a duty to exercise commercially reasonable methods and care in handling, using, maintaining, storing, and safeguarding the PII in its care,

control, and custody, including by implementing industry-wide standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and the unauthorized use that occurred, and to promptly detect and thwart attempts at unauthorized access to their networks and systems. This duty arose independently from any contract.

76. Defendant knew, or should have known, of the risks inherent in collecting and storing massive amounts of PII, including the importance of adequate data security and the high frequency of cyberattacks and well-publicized data breaches. Defendant owed duties of care to Plaintiff and Class Members because it was foreseeable that its failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that sensitive information. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and the Class Members' PII by failing to limit access to this information to unauthorized third parties and by not properly supervising both the way the PII was stored, used, and exchanged, and those in its employ responsible for such tasks.

77. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and Class Members the scope, nature, and circumstances of the Data Breach. This duty is required and necessary for Plaintiff and the Class to (1) take appropriate measures to protect their PII, (2) be vigilant in the face of an increased risk of harm, and (3) take other necessary steps to mitigate the harm caused by the Data Breach. As of the date of this filing, Defendant still has not disclosed the full nature and extent of the Data Breach to Plaintiff and Class Members, thereby depriving Plaintiff and Class Members of the opportunity to mitigate their own damages in a timely manner.

78. Defendant also had a common law duty to prevent foreseeable harm to others. Defendant had full knowledge of the sensitivity and high value of the PII that it stored and the types of foreseeable harm and injury-in-fact that Plaintiff and Class Members could and would suffer if that PII were wrongfully disclosed, leaked, accessed, or exfiltrated. Defendant's conduct created a foreseeable and unreasonable risk of harm to Plaintiff and Class Members, who were the foreseeable victims of Defendant's inadequate data security practices.

79. Defendant violated its duties to implement and maintain reasonable security procedures and practices. Defendant's duties also included, among other things, designing, maintaining, and testing its information security controls to ensure that the PII in its possession was adequately secured by, for example, encrypting or anonymizing sensitive personal information, installing intrusion detection and deterrent systems and monitoring mechanisms, and using access controls to limit access to sensitive data.

80. Defendant's duties of care also arose by operation of statute. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard the PII of Plaintiff and Class Members.

81. The FTC Act was enacted to protect Plaintiff and the Class Members from the type of wrongful conduct in which Defendant engaged.

82. Defendant breached its duties to exercise reasonable care in protecting Plaintiff's and Class Members' PII by failing to (1) implement and maintain adequate data security measures to safeguard Plaintiff's and Class Members' sensitive personal information, (2) encrypt or anonymize PII within its systems and networks, (3) monitor its systems and networks to promptly identify and thwart suspicious activity, (4) delete and purge PII no longer necessary for the provision of background check services to its clients and customers, as well as allowing unmonitored and unrestricted access to unsecured PII and allowing (or failing to prevent)

unauthorized access to, and exfiltration of, Plaintiff's and Class Members' confidential and private information. Additionally, Defendant breached its duties by utilizing outdated and ineffectual data security measures which deviated from standard industry best practices at the time of the Data Breach. Through these actions, Defendant also violated its duties under the FTC Act.

83. The law imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of PII to Plaintiff and Class Members so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuses of their PII. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class Members. In so doing, Defendant actually and proximately caused and exacerbated the harm from the Data Breach and the injuries-in-fact of Plaintiff and Class Members. Timely disclosure was necessary so that Plaintiff and Class Members could, among other things: (i) purchase identity theft protection, monitoring, and recovery services; (ii) flag asset, credit, and tax accounts for fraud; (iii) purchase or otherwise obtain credit reports; (iv) place or renew fraud alerts on a quarterly basis; (v) closely monitor loan data and public records; (vi) change or update passwords on their various accounts; and (vii) take other meaningful steps to protect themselves and attempt to avoid or recover from identity theft and other harms.

84. Defendant has the financial and personnel resources necessary to deploy robust cybersecurity protocols and controls, and to prevent the Data Breach, but nevertheless failed to adopt reasonable data security measures, in breach of the duties it owed to Plaintiff and Class Members.

85. Plaintiff and Class Members had no ability to protect their PII once it was in Defendant's possession and control. Defendant was in an exclusive position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

86. But for Defendant's breach of its duties to adequately protect Class Members' PII, Class Members' PII would not have been stolen. As a result of Defendant's negligence, Plaintiff and Class Members suffered and will continue to suffer the various types of damages alleged herein. There is a temporal and close causal connection between Defendant's failure to implement adequate data security measures, the Data Breach, and the harms suffered by Plaintiff and Class Members. Thus, Defendant is the factual cause of Plaintiff's and Class Members' harm.

87. Furthermore, Defendant is the proximate cause of Plaintiff's and Class Members' harm because the actions of third-party bad actors such as cybercriminals do not constitute a superseding force that would relieve Defendant from liability, as the misappropriation of PII for unlawful purposes by cybercriminals is an unambiguously foreseeable consequence of a steward of PII, such as Defendant, failing to adequately protect the data security of Plaintiff's and Class Members' PII.

88. As a direct and traceable result of Defendant's negligence, Plaintiff and the Nationwide Class have suffered or will suffer an increased and impending risk of fraud, identity theft, damages, embarrassment, humiliation, frustration, emotional distress, and lost time and out-of-pocket costs to mitigate and remediate the effects of the Data Breach. These harms to Plaintiffs and the Class Members include, without limitation: (i) loss of the opportunity to control how their personal information is used; (ii) diminution in the value and use of their personal information entrusted to Defendant; (iii) the compromise and theft of their personal information; (iv) out-of-pocket costs associated with the prevention, detection, and recovery from identity

theft and unauthorized use of financial accounts; (v) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including increased costs to use credit, credit scores, credit reports, and assets; (vi) unauthorized use of compromised personal information to open new financial and other accounts; (vii) continued risk to their personal information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the personal information in its possession; and (viii) future costs in the form of time, effort, and money they will need to expend to prevent, detect, contest, and repair the adverse effects of their personal information being stolen in the Data Breach.

89. Defendant's negligence was gross, willful, wanton, and warrants the imposition of punitive damages given the clear foreseeability of a hacking incident, the extreme sensitivity of the private information under Defendant's care, and its failure to take adequate remedial steps, including prompt notification to Class Members following the Data Breach.

90. Plaintiff and Class Members are entitled to all forms of monetary compensation set forth herein, including monetary payments to provide adequate long-term identity protection services. Plaintiff and Class Members are also entitled to the injunctive relief sought herein.

SECOND CAUSE OF ACTION
Negligence *Per Se*
(*On Behalf of the Plaintiff and the Nationwide Class Against Defendant*)

91. Plaintiff incorporates by reference and realleges paragraphs 1-73 as if fully set forth herein.

92. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to maintain fair and adequate computer systems and data security practices to safeguard Plaintiff's and the Nationwide Class' PII.

93. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duties to protect Plaintiff's and the Class Members' PII.

94. Defendant's duties to use reasonable care in protecting confidential and sensitive data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

95. Defendant violated its duties under Section 5 of the FTC Act by failing to use reasonable or adequate data security practices and measures to protect Plaintiff's and the Class Members' PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII that it collected and stored and the foreseeable consequences of a cybersecurity data breach, including, specifically, the immense damages that would result in the event of a breach, which ultimately came to pass.

96. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

97. But for Defendant's wrongful and negligent breach of the duties owed to Plaintiff and Class Members, Plaintiff and the Class Members would not have been injured.

98. The injuries and harms suffered by Plaintiff and the Class Members were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should

have known that it was failing to meet its duties and that the breach would cause Plaintiff and the Class Members to suffer the foreseeable harms associated with the exposure of their PII.

99. Defendant's various violations and its failure to comply with the applicable laws and regulations referenced above constitutes negligence *per se*.

100. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class Members have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII, entitling them to damages in an amount to be proven at trial.

101. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

THIRD CAUSE OF ACTION
Unjust Enrichment
(*On Behalf of the Plaintiff and the Nationwide Class Against Defendant*)

102. Plaintiff incorporates by reference and realleges paragraphs 1-73 as if fully set forth herein.

103. Plaintiff and Class Members had their PII collected by Defendant as part of its regular business of providing administration and processing services to the various debt settlement companies managing Plaintiff's and class members' consumer debt. Without Plaintiff's and Class Members' PII, Defendant could not conduct its regular business activities.

Thus, Plaintiff and Class Members conferred a pecuniary benefit to Defendant when they provided their PII to Defendant's clients—the various debt settlement companies.

104. Defendant knew that Plaintiff and Class Members conferred a pecuniary benefit to Defendant's clients and thereby Defendant, and Defendant accepted and retained that benefit. Defendant profited from this pecuniary benefit as its clients must transmit Plaintiff's and Class Members' PII to Defendant as an essential part of Defendant's business. Without Plaintiff's and Class Members' PII, Defendant would not be able to offer administration and processing services for debt settlement companies and therefore would not make a profit.

105. Under principles of equity and good conscience, Defendant should not be permitted to retain the pecuniary benefit it gained from collecting Plaintiff's and Class Members' PII because Defendant failed to adequately safeguard that PII by not implementing or paying for reasonable and standard cybersecurity procedures and protocols.

106. Plaintiff and the Class Members have no adequate remedy at law. Defendant continues to retain their PII while exposing this sensitive and private information to a risk of future data breaches while in Defendant's possession. Defendant also continues to derive a financial benefit from using Plaintiff's and Class Members' PII.

107. As a direct and proximate result of Defendant's wrongful conduct, Plaintiff and Class Members have suffered various types of damages as alleged herein.

108. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by it because of its misconduct described herein and the Data Breach.

FOURTH CAUSE OF ACTION
Invasion of Privacy
(*On Behalf of the Plaintiff and the Nationwide Class Against Defendant*)

118. Plaintiff incorporates by reference and realleges paragraphs 1-73 as if fully set forth herein.

119. Plaintiff and Class Members have a legally protected privacy interest in their PII, which is and was collected, stored, and maintained by Defendant, and they are entitled to the reasonable and adequate protection of their PII against foreseeable unauthorized access, as occurred with the Data Breach.

120. Plaintiff and Class Members reasonably expected that Defendant would protect and secure their PII from unauthorized parties and that their private information would not be accessed, exfiltrated, and disclosed to any unauthorized parties or for any improper purpose.

121. Defendant unlawfully invaded the privacy rights of Plaintiff and Class Members by engaging in the wrongful conduct described above, including by failing to protect their PII by permitting unauthorized third parties to access, exfiltrate, and view this private information. Likewise, Defendant further invaded the privacy rights of Plaintiff and Class Members and permitted cybercriminals to invade the privacy rights of Plaintiff and Class Members, by unreasonably and intentionally delaying disclosure of the Data Breach, and by failing to properly identify what PII had been accessed, exfiltrated, and viewed by unauthorized third parties.

122. This invasion of privacy resulted from Defendant's failure to properly secure and maintain Plaintiff's and the Class Members' PII, leading to the foreseeable unauthorized access, exfiltration, and disclosure of this unguarded data.

123. Plaintiff's and the Class Members' PII is the type of sensitive, personal information that one normally expects will be protected from exposure by the very entity charged with safeguarding it. Further, the public has no legitimate concern in Plaintiff's and the Class Members' PII, and such private information is otherwise protected from exposure to the public by various statutes, regulations, and other laws.

124. The disclosure of Plaintiff's and the Class Members' PII to unauthorized parties is substantial and unreasonable enough to be legally cognizable and is highly offensive to a reasonable person.

125. Defendant's willful and reckless conduct which permitted unauthorized access, exfiltration and disclosure of Plaintiff's and the Class Members' sensitive PII is such that it would cause serious mental injury, shame, embarrassment, or humiliation to people of ordinary sensibilities.

126. The unauthorized access, exfiltration, and disclosure of Plaintiff's and the Class Members' PII was without their consent, and in violation of various statutes, regulations, and other laws.

127. As a result of the invasion of privacy caused by Defendant, Plaintiff and the Class Members suffered and will continue to suffer damages and injuries as set forth herein.

128. Plaintiff and the Class Members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution, injunctive relief, reasonable attorneys' fees and costs, and any other relief that the Court deems just and proper.

FIFTH CAUSE OF ACTION
Injunctive / Declaratory Relief
(*On Behalf of the Plaintiff and the Nationwide Class Against Defendant*)

129. Plaintiff incorporates by reference and realleges paragraphs 1-73 as if fully set forth herein.

130. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal statutes described herein.

131. Defendant owes a duty of care to Plaintiff and Class Members, which required Defendant to adequately monitor and safeguard Plaintiff's and Class Members' PII.

132. Defendant and its officers, directors, affiliates, legal representatives, employees, co-conspirators, successors, subsidiaries, and assigns still possess the PII belonging to Plaintiff and Class Members.

133. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and whether Defendant is currently maintaining the data security measures adequate to protect Plaintiff and Class Members from further data breaches that may again compromise their PII. Plaintiff alleges that Defendant's data security measures remain inadequate. Furthermore, Plaintiff and the Class Members continue to suffer injury as a result of the compromise of their PII and the risk remains that further compromises of their private information will occur in the future.

134. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to adequately secure the PII of Plaintiff and the Class Members within its care, custody, and control under the common law and Section 5 of FTC Act;

b. Defendant breached its duties to Plaintiff and the Class Members by allowing the Data Breach to occur;

c. Defendant's existing data monitoring measures do not comply with its obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect the PII of Plaintiff and the Class Members within Defendant's custody, care, and control; and

d. Defendant's ongoing breaches of said duties continue to cause harm to Plaintiff and the Class.

135. This Court should also issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with data broker industry standards to protect the PII of Plaintiffs and the Class within its custody, care, and control, including the following:

a. Order Defendant to provide lifetime credit monitoring and identity theft insurance and protection services to Plaintiff and Class Members; and

b. Order that, to comply with its obligations and duties of care, Defendant must implement and maintain reasonable security and monitoring measures, including, but not limited to:

i. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems, networks and servers on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third party security auditors;

ii. Encrypting and anonymizing the existing PII within its servers, networks, and systems to the extent practicable, and purging all such information which is no longer reasonably necessary for Defendant to provide adequate background check services to its clients and customers;

iii. Engaging third-party security auditors and internal personnel to run automated security monitoring;

iv. Auditing, testing, and training its security personnel regarding any new or modified procedures;

v. Segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems, networks, and servers;

vi. Conducting regular database scanning and security checks; and

vii. Routinely and continually conducting internal training and education to inform Defendant's internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

136. If an injunction is not issued, Plaintiff and the Class Members will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach or cybersecurity incident. This risk is real, immediate, and substantial. If another data breach or cybersecurity incident occurs at Defendant, Plaintiff and the Class Members will not have an adequate remedy at law because monetary relief alone will not compensate them for the serious risks of future harm.

137. The hardship to Plaintiff and Class Members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Plaintiff and Class Members will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Defendant's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

138. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach or cybersecurity incident, thus preventing future injury to Plaintiff, Class Members and other persons whose PII would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Nationwide Class sets forth herein, respectfully requests the following relief:

A. Certifying this action as a class action under Fed. R. Civ. P. 23 and appointing Plaintiff and his counsel to represent the Class;

B. Entering judgment for Plaintiff and the Class;

C. Granting permanent and appropriate injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein and directing it to adequately safeguard the PII of Plaintiff and the Class by implementing improved security controls;

D. Awarding compensatory, consequential, and general damages, including nominal damages, as appropriate and as allowed by law in an amount to be determined at trial;

E. Award statutory or punitive damages and penalties as allowed by law in an amount to be determined at trial;

F. Ordering disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendant as a result of its unlawful acts, omissions, and practices;

G. Awarding to Plaintiff and Class Members the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

H. Awarding pre- and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper; and

I. Granting such further and other relief as may be just and proper.

DEMAND FOR TRIAL BY JURY

Plaintiff hereby demands a trial by jury.

Dated: November 25, 2024

Respectfully submitted,

/s/James C. Shah

James C. Shah
Alec J. Berin
MILLER SHAH LLP
2 Hudson Place, Suite 303
Hoboken, NJ 07030
Telephone: (866) 540-5505
Facsimile: (866) 300-7367
jcshah@millershah.com
ajberin@millershah.com

Amber L. Schubert*
SCHUBERT JONCKHEER & KOLBE LLP
2011 Union St., Suite 200
San Francisco, CA 94123
Telephone: (415) 788-4220
Facsimile: (415) 788-0161
aschubert@sjk.law

Counsel for Plaintiff David Jacob and the Putative Class

**pro hac vice* to be filed